Appendix D
System Administration

1 CPAIS SYSTEM ADMINISTRATOR

The CPAIS System Administrator ensures that all system components are available to effectively meet the needs of the CPAIS users. The system administrator must implement CPAIS standards related to system management, along with all amendments that may be produced to take advantage of features offered by new technology. Activities also include developing security contingency plans and monitoring system security.

1.1 System Administrator Duties

- Assesses existing computer resources and identifies additional needs.
- Develops guidelines and offers consultation for optimal computer configurations.
- Determines the on-line storage capacity, computer memory, server, workstation, and PC configuration for the processing and management of data.
- Monitors computer resources and makes recommendations for changes to the system.
- Ensures that the systems are kept running and maintained with the latest technology.
- Monitors and tunes the system to improve performance.
- Loads data onto the system and ensures its security.
- Provides security for corporate data via user access control.
- Provides access for maintenance of corporate data.
- Performs scheduled backups of the data.
- Archives historical data.

1.2 System Administrator Coordination Responsibilities

- Coordinates with the Database Administrator and Data Stewards to understand the nature and size of the data sets.
- Coordinates with the Database Administrator and Data Stewards to ensure backups and archives are performed when necessary.
- Works with the Database Administrator and Data Stewards to ensure needed security and data access.
- Coordinates with all individuals involved in the process to ensure that systems are meeting project and organizational needs.
- Coordinates with the Network Manager to ensure all systems can communicate with each other.

2 USER ACCESS

This section defines the various functions that users will perform in CPAIS and describes the access responsibilities of users and supervisors. The complete procedures and user access request forms can be found in the CPAIS Operations Guide.

2.1 User Roles

There are a number of user roles required to administer CPAIS. These roles are:

- The ***Real Property Manager*** creates and maintains the property sub ledger and sets developments status.
- The ***Real Property Disposal Manager*** creates and updates the sub ledger. He or she also creates write off transactions for disposal of assets.
- The ***Real Property Stream Manager*** creates and updates prior year adjustments.
- The ***Real Property HQ Manager*** creates and updates the CPAIS accounting codes tables.
- The ***GSA Manager*** creates, updates, and deletes access to GSA site data.
- The ***Property/Fiscal/Facility Engineer*** links owned properties to GSA sites.
- The ***Lease Manager*** creates, updates, and deletes leases. He or she also issues GSA OA bill adjustments.

2.2 User Access and Responsibilities

Access to the "Create, Update, Delete" function is carefully controlled by Oracle roles. Different resource staff will have access to different parts of CPAIS for different purposes. The needed role must be specified on the "User Access, Update, Revocation Request – Application" form (See G-10). This form covers the duration of each user to CPAIS. The same form and procedure is to be used to add new users and to change or revoke access for current users.

In addition to roles, fine-grained security is used to limit user access to specifically requested organizations (i.e., admin org). Admin orgs must also be specified on the form as part of the request.

Users and supervisors have distinct responsibilities as they relate to user access privileges. The User Management process is handled through forms that contain user information, the role that is needed, and the adminorgs to which access is needed. Access to CPAIS is provided once the "User Access, Update, Revocation Request – Application" Replace with 1143 form is approved by the supervisor and approved by the ACFO-FS.

This form is forwarded via e-mail to the CPAIS System Administrator where the request is processed. Only forms, that have been sent from the requesting agency's financial management or property management organization, are considered valid. Forms coming directly from users or any other source outside the process will be processed. Once approved, the system administration staff will process the request. It is important that supervisors request the revocation of privileges for user accounts when their subordinates change job responsibilities or leave the employment of USDA.

2.3 Processing of Valid Requests

The CPAIS System Administrator reviews and processes new or update profile requests by validating the user id, creating a new CPAIS user, granting the appropriate roles, adding user information into the fiscal user table, and entering or updating the requested location(s) for the user.

"Revoke" requests are processed by dropping the CPAIS user logon and password, and removing the user information from the fiscal user and user access tables.

2.4 Aging of Passwords

User accounts are disabled when the password has not been changed within 60 days. Accounts are disabled by revoking the connect role from the user account. Accounts are re-enabled by placing a request to the help desk and opening a help desk ticket.

2.5 Restriction of Access

When notification has been given that a user no longer needs access to CPAIS from the quarterly user review report or e-mail (e.g., a request from the user asking to be removed from the mailing list because that is no longer part of their job), the account can be restricted by revoking connect privileges pending processing of the revocation request on the Access Request Form (1143).

2.6 Monthly User Access Report

The monthly user access report is used to inform management with notification of user accounts that have been added or removed within the last month. A list of users is provided with the time-stamp of the last system access by the user. In addition, users who have restricted accounts are flagged on the report.

The monthly user access report is for user tracking only and responses are not required. Supervisors are expected to review the Monthly User Access Report. An example of this report is provided below:

MONTHLY USER ACCESS REPORT -- Example

```
USER_NAME    CONTACT          EMAIL                PHONE_NUMBER       AGENCY_CODE
------------ ---------------- -------------------- ------------------ ------

ASPEER       ANN SPEER        ASPEER@FS.FED.US     406-329-4974       1223
LAST ACCESS DATE: 08-AUG-2003

 ROLES: II_RPA_DISPOSAL_MGR
 ORGS: 01, 0152, XXXX

TEKART       TANYA EKART      TEKART@FS.FED.US     710-250-4463 x113  1223

 LAST ACCESS DATE: 10-AUG-2003

 ROLES: II_RPA_DISPOSAL_MGR
 ORGS: 0108, 0118, XXXX

SSMITH       SAM SMITH         SSMITH@FS.FED.US    555-555-5512       1223

 ** NEW USER **
 LAST ACCESS DATE: 20-AUG-2003

 ROLES: II_RPA_DISPOSAL_MGR
 ORGS: 02, XXXX
```

Supervisors and area coordinators must also conduct a quarterly user review. During this review, supervisors and area coordinators must examine the Quarterly User Review report to verify that the list of users and access status is valid. An example of this report is provided below:

QUARTERLY USER REVIEW REPORT -- Example

Users added during this quarter: 4
Users removed during this quarter: 1

List of users added during this quarter: Use some usda.gov addresses!!

```
AJONES        ALAN A JONES     AASMITH@FS.FED.US
BSMITH02      BRENDA J SMITH   BSMITH02@FS.FED.US
CREYNOLDS     CINDY REYNOLDS   CREYNOLDS@FS.FED.US
SSMITH        SAM C SMITH      SSMITH@FS.FED.US
```

List of users removed during this quarter:

```
CMILLER       CINDY R MILLER   CMILLER@FS.FED.US   555-555-1222
```

Current List of Users by Supervisor:

```
1) APARHAM    APARHAM@FS.FED.US    555-555-1223
       a) AJONES        ALAN A JONES     AASMITH@FS.FED.US
       b) BSMITH02      BRENDA J SMITH   BSMITH02@FS.FED.US
       c) CREYNOLDS     CINDY REYNOLDS   CREYNOLDS@FS.FED.US

2) ASPEER        ANN SPEER        ASPEER@FS.FED.US    406-329-4974      1223
       a) SSMITH        SAM C SMITH      SSMITH@FS.FED.US
```

Supervisors and areas coordinators are expected to formally respond to their review of this report.

3 HELP DESK

The CPAIS Help Desk has several responsibilities related to supporting the users of CPAIS. First, the help desk must respond to user access problems such as a locked-out user account or forgotten password. The help desk staff will unlock the user account and change the user's password as appropriate.

The Help Desk staff must also respond to user problems and system errors. The staff will solve problems immediately, if possible, or assign the problem to the appropriate resource if they cannot solve the problem.

Finally, the staff must monitor the system for script errors. CPAIS script errors processing is automated. Consequently, an error will send an automatic alert to on-call staff.

Refer to the CPAIS Operations Guide and Help Desk Guide for full procedures for supporting CPAIS and resolving problems.

4 SECURITY ADMINISTRATION

CPAIS is not a classified system, however, the information is sensitive and must be protected. The CPAIS System Administrator works with the Agency and Department Security staff to ensure security of the information in CPAIS in accordance with Federal and Departmental Regulations. Additionally, the System Administrator monitors compliance with the security provisions of the CPAIS as documented in the System Security section of CPAIS Design Document and all other relevant documents.

4.1 Security Officer

The CPAIS Security Officer (CSO) is responsible for the security of all CPAIS configuration components including database, mail, and application servers. The CSO, in conjunction with the system administrator, monitors user activity to ensure proper compliance with applicable security regulations and security guidance. The CSO performs initial evaluation of security problems. The CSO conducts security-training, reviews proposed configuration changes for security implications and documents security vulnerabilities and incidents.

4.2 Security Administrator

The CPAIS system administrator administers user accounts, including new user creations, access changes, and access revocations. System administrators also monitor user activity, update user account information, review audit logs, and check for expired passwords.

5 SYSTEM MAINTENANCE

A variety of tasks are required to maintain CPAIS. These tasks are described below. This section identifies and describes these activities.

5.1 Routine Backups

Daily backups of the CPAIS software and data are needed to ensure system integrity in the event of an error. Several types of backups are created at different increments of the month. On the Unix-based database server, database extracts are taken daily, cold backups (which require the database to be down) are taken weekly, and a full system backup is taken monthly. Refer to the CPAIS Operations Manual for complete instructions on backup and restore procedures.

5.2 Performance Monitoring and Tuning

CPAIS system administrator must continuously monitor the performance of CPAIS. Performance elements requiring monitoring include the network on which CPAIS resides, the CPAIS application, the CPAIS database, and the CPAIS hardware. When performance issues are identified, the system administrator is responsible for identifying

the source of the problem and assigning the appropriate resources to resolve the problem. Performance problems may require the help of outside vendors such as Database Management System (DBMS) providers.

5.3 Upgrades

CPAIS elements must be periodically upgraded to implement new features and ensure up-to-date technology is employed. Upgrades fall into four major categories. These are:

- Application: Application upgrades add new features or fix known problems.
- Database: Database upgrades will update the DBMS used by CPAIS with the latest version provided by the DBMS vendor.
- Hardware: Hardware upgrades may be necessary to improve performance.
- Operating system: Operating system upgrades are necessary to implement patches that fix known problems such as security vulnerabilities. These are also necessary to keep the CPAIS platform up to date.

5.4 Managing External Interfaces

There are a number of external interfaces to the CPAIS application that provide for exchange of data between systems. These systems are FFIS, GSA STAR, FS INFRA, and GSA FRPP. The System Administrator will manage and monitor the processing of these interfaces.

The System Administrator will review logs and reports that are generated by the interface processing procedures on a daily basis. Any discrepancies and errors that are found and documented will be reported to the database administrator and the system administrator of the originating system. The CPAIS System Administrator will initiate remedial action and ensure that the errors are corrected and the interfaces are refreshed with correct data.

5.5 Disaster Recovery

Recovery is accomplished through the recovery process defined at NITC. Complete database recovery can be performed by restoring files from the cold database backups. Complete system recovery can be done to the original system or to a compatible system using the full monthly system backup tapes. The latest database cold backup can then be restored to have the most recently backed-up version of the database. The database recovery process must follow recovery procedures set by Oracle.

5.6 Maintenance of Reference Tables and List of Values

The System Administrator, in conjunction with the DBA, will be responsible for maintaining and updating the CPAIS reference tables and lists of values. The System

Administrator must follow the steps described below to ensure proper and correct updating of the tables and lists.

- Develop a form, (or modify an existing form to correspond with the needs of CPAIS), for requesting changes to reference tables and lists of values.
- Receive request for modification to the values.
- Verify and validate that the new value meets all prevailing standards and conventions.
- Verify and validate the acceptance of the new value by the Department Data Steward, OCFO, all agencies and staff offices, and GSA, if applicable.
- Ensure that the new/changed value will not interfere with or duplicate any other values in the table or list.
- Consult with the DBA if the same value appears in other tables with or without the same description.
- Review interface documents to ensure that there are no conflicts between values transferred between the systems.
- Inform all users and developers of the update.
- Access the Oracle Forms that allow "Create, Update, Delete" functions for specified tables and lists.
- Make appropriate updates.

6 DATABASE ADMINISTRATION

Administration, maintenance, and management of the CPAIS database is the responsibility of the Database Administrator. The database administrator (DBA) supports the development and use of database systems. The DBA must focus on the detailed needs of the individual users and applications, performing database tuning when necessary, to ensure efficient input, update, and retrieval of data. The DBA works closely with the system administrator to ensure the physical environment is conducive to design, development and implementation of database systems. This position provides database administration support for all applications.

6.1 Database Administrator

The Database Administrator has the following duties:

- Works closely with the system administrator to ensure the physical environment is conducive to design, development and implementation of database applications, (e.g., identifying appropriate physical space, networking, and access criteria).
- Coordinates the development and implementation of procedures that ensure data consistency, integrity and quality with the data steward.
- Builds a data structure conducive to an enforcement of standards as developed at the system level of data administration and by data stewards. Although the ultimate responsibility for identification of standards related to the data and processes resides with the data steward, it is the responsibility of the DBA to build a data structure conducive to the enforcement of these standards.
- Performs database tuning to ensure efficient input, update, and retrieval of data.
- Monitors the data set and application usage and routinely reports back to the Data Steward regarding the use of a particular data set or application.
- Ensures the data set is readily available for sharing, both internally and externally.
- Coordinates the identification, assessment of impacts, strategy and implementation of change management procedures for a data set.
- Implements appropriate data security measures by aiding in the control of access at several levels. Works closely with the system administrator to ensure this security exists at the appropriate levels (network, platform, data, and application).
- Assesses current and new technology merit (e.g., new technology tool performance, cost of change ramifications at all levels, etc).

6.2 Database Administration Coordination

The database administration coordinator has the following responsibilities:

- Coordinates with project sponsors and data stewards to design and develop a data structure that meets their needs.
- Coordinates with system administrators and other information support to ensure adequate physical environment and system security.
- Coordinates the identification, impact assessment, strategy and implementation of the "change management" procedures for the data set.

Attachment

Replace with the 1143!!!!!